Children's Charities' Coalition on Internet Safety

Digital manifesto

Fourth edition 2015

Contents

About the Children's Charities' Coalition on Internet Safety

The Children's Charities' Coalition on Internet Safety (CHIS) is made up of representatives from Action for Children, Barnardo's, the British Association for Adoption and Fostering, Children England, The Children's society, ECPAT UK, Kidscape, National Children's Bureau, The National Society for the Prevention of Cruelty to Children, Stop It Now UK and Ireland, and Young Minds.

CHIS members provide a comprehensive range of expertise in child protection, child welfare and child development. The information presented here reflects the experience and extensive professional knowledge of the member organisations.

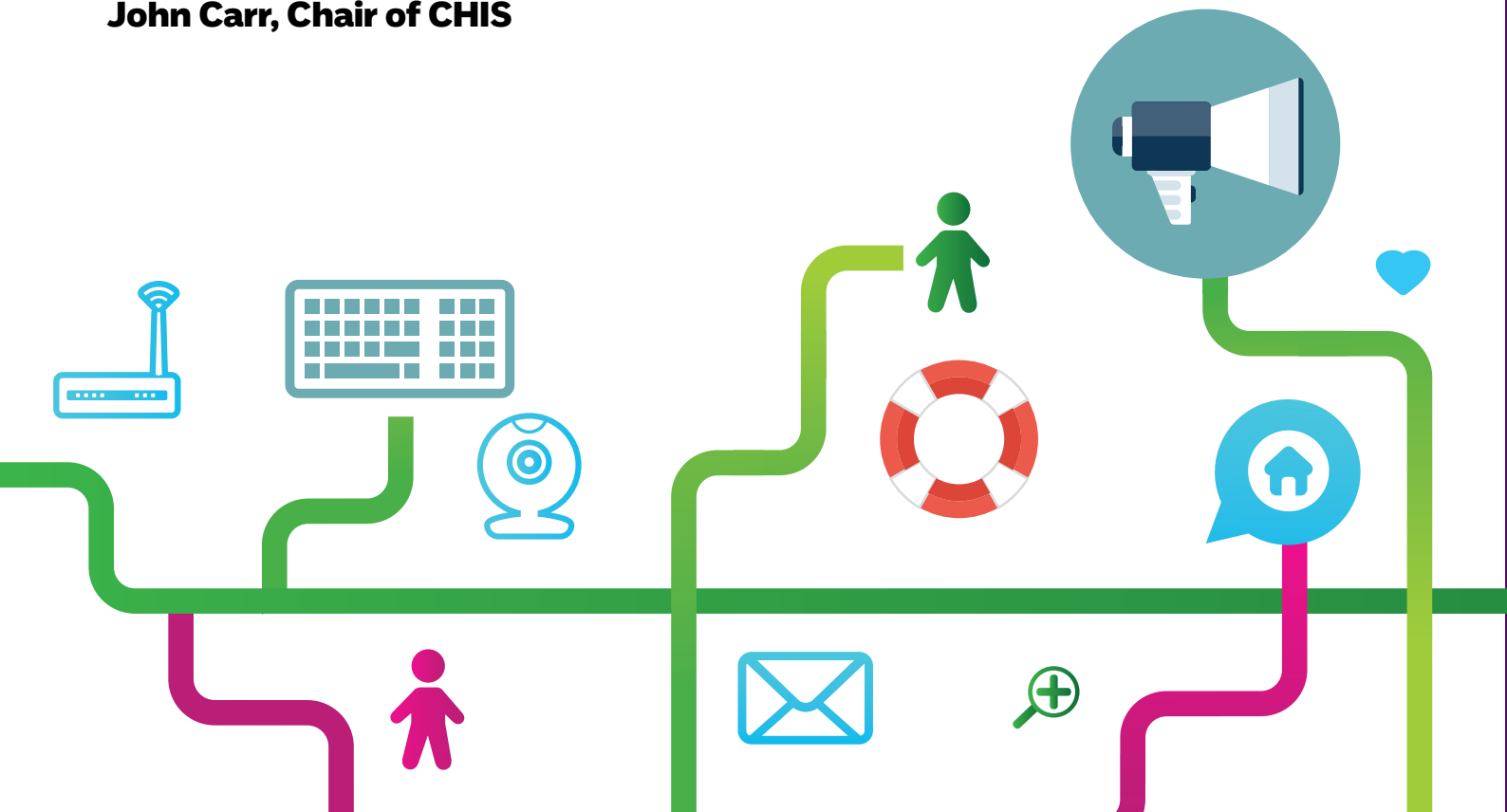
Why a digital manifesto?

The general election scheduled for May 2015 will soon be upon us. With that in mind the Children's Charities' Coalition on Internet Safety (CHIS) here presents its digital manifesto, which is being sent to all of the major political parties.
The first CHIS manifesto appeared before the general election in 2001. Updated versions were also published before the elections in 2005 and 2010.

CHIS asks that all political parties commit themselves to supporting the policies we are putting forward. Responses received will be published on our website (www.chis.org.uk).

There has been a substantial degree of consensus between the major parties on all matters connected with online child safety. We earnestly hope that, whatever the outcome of the 2015 general election, this position will continue throughout the life of the next parliament. We have every reason to believe it will.

John Carr, Chair of CHIS



Summary of principal recommendations

1. The government should consider creating a new legal right for victims of child sex abuse to obtain financial compensation from persons found in unlawful possession of an image of that abuse.

2. It should be made a crime for any bank, credit card company or other organisation to provide financial or other services to websites involved in the commercial publishing of pornography without having a robust age verification mechanism in place to ensure children cannot access it.

3. The same principle should be extended to all businesses selling any type of legally age-restricted goods or services over the internet.

4. A new body should be established, or a new division created within an existing one, with the legal powers to ensure internet companies are transparent and accountable in respect of actions aimed at supporting online child safety, and in particular in relation to potential sexual abuse or content that encourages damaging behaviour.

5. Such a body or division should also be given the power to make legally binding orders requiring internet companies to take necessary and proportionate measures to safeguard children online, both generally and in respect of their position as economic actors and targets of advertising.

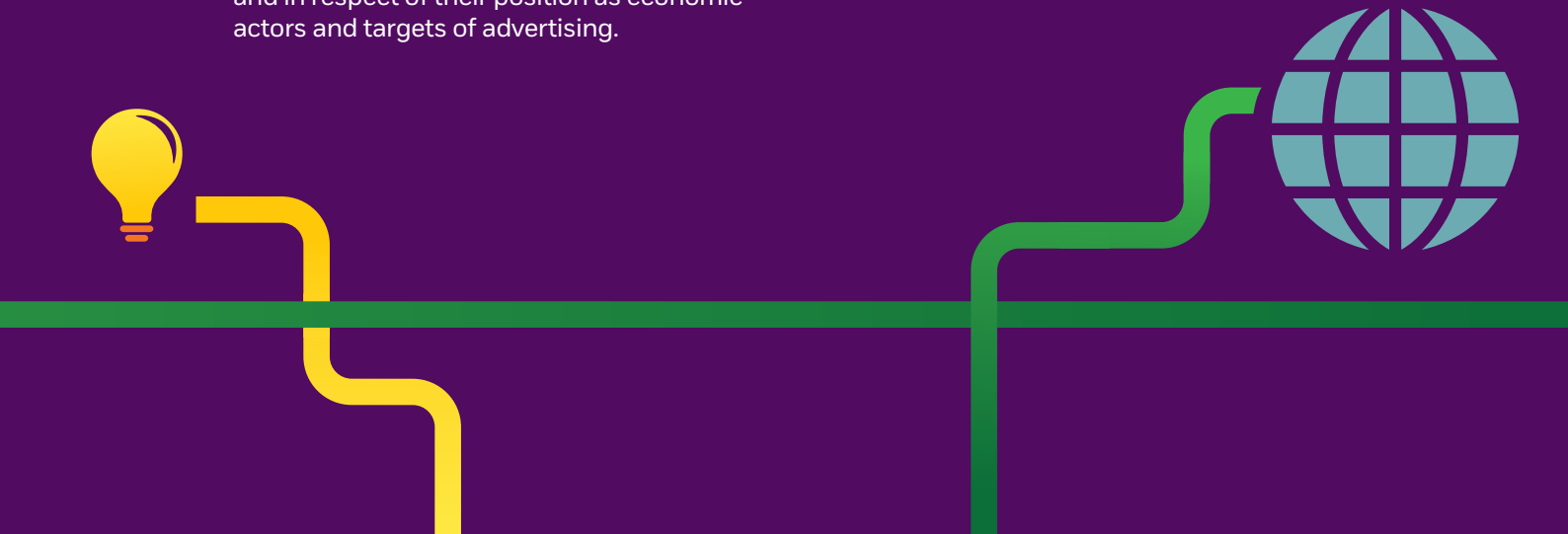
6. Every UK territorial police force should have a dedicated unit with appropriately trained officers to deal specifically with sexual and other online offences against children.

7. A major review of public policy in respect of child abuse images online should be established.

8. The next government should take the lead in establishing an international body to mediate between industry and law enforcement in relation to illegal online content to ensure it is identified and removed from the internet rapidly.

9. The next government should press for an amendment to, or clarification of, the E-Commerce Directive to ensure it does not act as a disincentive to firms actively seeking out content or activity on their sites which breaches their terms and conditions of service.

10. The next government should establish a 'high-tech social fund', financed through corporate contributions, to support research into online child protection and the deterrence of online offenders, as well as initiatives to support children who have been the victims of abuse online.



Making the internet safer for children – progress from 2010-15

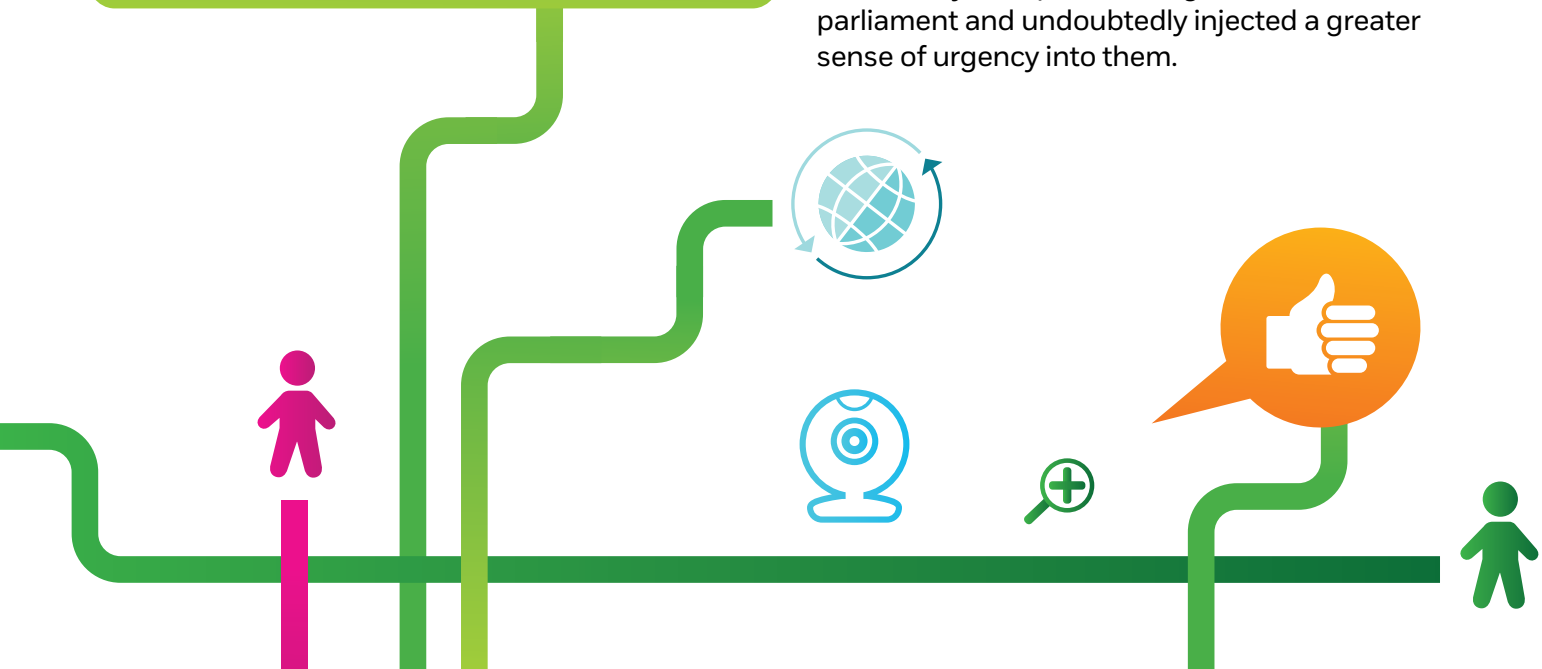
This manifesto restricts itself to examining the online dimensions of public policy insofar as they concern children and young people's use of technology and the internet.

In June 2010, just over a month after the last General Election, with memories of the Baby P case still fresh in everyone's minds, the Secretary of State for Education, Michael Gove, appointed Professor Eileen Munro to carry out a review of England's child protection system. In December 2010, Mr Gove asked Reg Bailey to initiate an enquiry into the "the commercialisation and sexualisation of childhood".

From the very beginnings of the last parliament, it was clear that children's health and welfare were going to continue to feature prominently in political and wider policy debates.

That said, in the latter part of 2010, few people could have anticipated the extent to which concerns about child abuse would come to dominate public discourse. Organised grooming and abuse in Rotherham, Rochdale, Oxford and elsewhere came to light. The police made disclosures about the volume of online offending against children, and the murders of April Jones and Tia Sharp shocked the nation. All of these things happened alongside the revelation of the unprecedented scale of child sex abuse carried out by Jimmy Savile and other celebrities, prompting the formation of Operation Yewtree and a promise from the government to establish an independent review into child sexual abuse and exploitation in the UK.

All of these events contributed to the disturbing backdrop against which discussions about online child safety took place during the 2010-15 parliament and undoubtedly injected a greater sense of urgency into them.



The Bailey Review

This built upon and extended the Byron Review, which had been commissioned by the previous government. In June 2011, The Bailey Review reported three recommendations directly addressing children's and young people's engagement with the internet. Several of the others resonated in or with cyberspace to varying degrees.

The three recommendations specific to the internet involved calls to:

1. Make it easier for parents to block adult and age-restricted material from the internet.
2. Prohibit the employment of children as brand ambassadors and in peer-to-peer marketing.
3. Ensure greater transparency in the regulatory framework by creating a single website for regulators.

The first recommendation is a mighty undertaking – the first of its kind in the democratic world. The UK's four largest Internet Service Providers (ISPs) – BT, Sky, Talk Talk and Virgin, which between them have around 90 per cent of the domestic broadband market – have completed or will be nearing completion of rolling out a set of tools for parents to protect children from age-inappropriate online content. These ISPs also embarked on a three-year programme to educate parents about online safety generally, and in particular how technical tools can and cannot play a role in keeping children safe online.

A key part to the ISPs' strategy was the creation of the online portal www.internetmatters.org. In the main body of the manifesto, we make clear that we think this is a brave experiment that we fully support. But, while the industry's efforts deserve to be recognised and applauded, it remains to be seen how effective the initiative will be and what lessons we will learn from it. Moreover, since the smaller ISPs share approximately 10 per cent of the broadband market – too large a proportion to ignore – it is important to see whether, or to what extent, they follow the lead of the "Big Four".

Recommendation two was achieved through an industry agreed standard adopted by the Advertising Association. [1]

Recommendation three was implemented with minimal central government engagement or expenditure by several agencies cooperating to establish ParentPort, although it has been reported that parents' awareness and use of the site is limited.[2] This should be regarded as a missed opportunity for child online safety. The evidence suggests that the vast majority of parents take some sort of action to mediate their child's use of online content and services, but many want and need more support to do so. For example, large numbers of parents, particularly of older children, agree with the statement "My child knows more about the internet than I do." [3]

[1] http://www.check.uk.com/ [accessed February 15 2015]

[2] Reg Bailey reported on the Mothers' Union website that "research published by the Chartered Institute of Marketing in June 2012 showed that 85 per cent of parents remained unaware of ParentPort" http://www.mothersunion.org/ensuring-core-parenting-skills-online-%E2%80%93-and-offline#sthash.LEII2RQ8.dpuf

[3] Ofcom, *Children and Parents: Media Use and Attitude Reports* [Online], October 2014, http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-use-attitudes-14/Childrens_2014_Report.pdf [accessed 17 February 2015]

Tackling child abuse images online

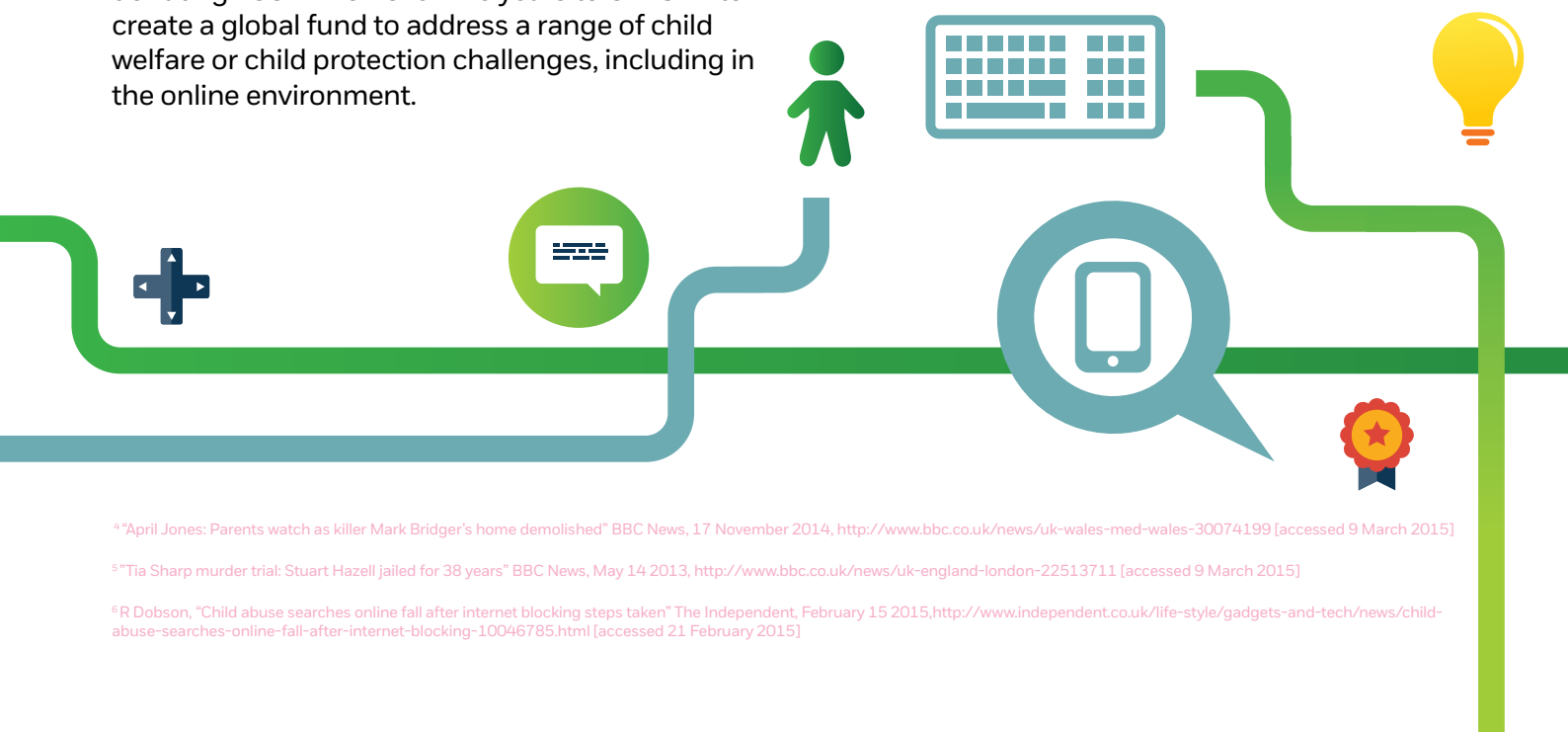
Following the murders of April Jones[4] and Tia Sharp[5], and in particular following the trials and convictions of their murderers in October 2012 and May 2013, there was a huge focus on how search engines and other parts of the internet were being used by paedophiles in order to locate child abuse images and other paedophilic materials. This led to Google and Microsoft making major changes to how their search tools worked. In January 2015, it was reported that these had led to a "precipitous drop" in the volume of searches for child abuse images on those platforms.[6]

More broadly, the government created and convened We Protect Children Online, an industry working group that is developing a series of proposals to add to the existing armoury of child protection measures.

In December 2014, the government convened a global conference to discuss progress with the We Protect initiative. At the conference the Prime Minister announced that the government was donating £50 million over five years to UNICEF to create a global fund to address a range of child welfare or child protection challenges, including in the online environment.

Also in December 2014, the prime minister announced the creation of a new joint unit consisting of GCHQ and the National Crime Agency (NCA). It will mainly target paedophiles operating on the 'darknet'. An extra £10 million was also promised to the NCA to create additional specialist online child sexual abuse teams focusing on the worst online offenders.

In the past five years, the Internet Watch Foundation's (IWF) legal powers and budgets have been significantly expanded. The main providers of public WiFi have all agreed to block access to known child abuse websites and, in respect of legal pornography, to sites in public spaces where children are likely to be found. In the Serious Crime Act 2015 there are clauses which make so called pedophiles manual illegal and also make it illegal for a adult to send a sexual message to a child.



[4] "April Jones: Parents watch as killer Mark Bridger's home demolished" BBC News, 17 November 2014, http://www.bbc.co.uk/news/uk-wales-med-wales-30074199 [accessed 9 March 2015]

[5] "Tia Sharp murder trial: Stuart Hazell jailed for 38 years" BBC News, May 14 2013, http://www.bbc.co.uk/news/uk-england-london-22513711 [accessed 9 March 2015]

[6] R Dobson, "Child abuse searches online fall after internet blocking steps taken" The Independent, February 15 2015,http://www.independent.co.uk/life-style/gadgets-and-tech/news/child-abuse-searches-online-fall-after-internet-blocking-10046785.html [accessed 21 February 2015]

Protecting children from inappropriate content

A change was made to the Video Recordings Act to lower the threshold at which previously exempt videos, such as music, sport or educational videos, lose their exemption from classification. From October 2014, all videos unsuitable for under 12s will require classification by the British Board of Film Classification (BBFC) to guide consumers and keep inappropriate content away from children. The UK Music industry has also agreed to trial a scheme with the BBFC, which would lead to music videos being classified. This would provide information to parents and consumers about the nature of the content, although an issue remains to be resolved where the artist concerned is domiciled overseas.

An amendment to the Communications Act 2003 came into effect in December 2014. This more closely aligns online and offline protections for children with regard to potentially harmful content. Any content classified by the BBFC as 'R18' must be placed behind access controls on UK-regulated video-on-demand services. This normally covers material that can only be sold on DVDs in licensed sex shops. Any content the BBFC refuses to classify must be banned from those services. The BBFC, Association of Television on Demand (ATVOD) and Ofcom signed a memorandum of understanding to give practical effect to this legislative change. However, this still leaves the issue of how to deal with content published on websites that are not subject to UK law unresolved.

In October 2014, Ofcom published new data showing the extent to which children and young people have adopted portable devices.[7] There has been a significant increase in access to, ownership of and use of tablet computers by children of all ages. Almost twice as many children aged 5-15 go online via a tablet than in 2013. In contrast, the incidence of TVs and games consoles in the bedroom is declining. Smartphone ownership is steady, though children are more likely to go online using a mobile phone than ever before.

On 8 December 2014, only a matter of days before he stood down after eight years as CEO of Ofcom, Ed Richards gave a speech at an event in Parliament. He spoke about the large scale, imminent arrival of internet enabled television sets in family living rooms and children's bedrooms that would inevitably raise a whole new set of challenges for the industry and public policy-makers. For that, and other reasons, Richards expressed his "firm belief" that in relation to the internet, the UK's regulatory framework is therefore still very much a work in progress. We agree.[8]

It is clear that during the 2010-15 parliament there was a great deal of activity designed to make the internet a safer place for children. CHIS will continue to track the efficiency of these measures, but there are a number of additional measures which we urge the next parliament to consider in order to improve online child safety.

[7] Ofcom *Children and Parents: Media Use and Attitude Reports* [Online], October 2014, http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-u14/Childrens_2014_Report.pdf [accessed 21 February 2015]

[8] Access to smart TVs by children has increased, from 13 per cent of 5-15s in 2013 to 39 per cent in 2014. Ibid.

The internet, children and young people – an overview

No one company or agency has a monopoly of knowledge, wisdom or expertise in online safety. Providing a safe environment on the internet for children and young people is a shared responsibility. Parents and those who look after children will always be a child's best and first source of guidance and support, but many of these people find the internet difficult to navigate and understand. We can not simply insist that it is down to parents, carers and schools to meet children's needs.

It should be noted that under the terms of the United Nations Convention on the Rights of the Child all signatory governments, including the UK, have accepted the legal obligation to ensure that all of the rights accorded to children by the Convention are honoured. The iRights coalition[9], a group of nearly 100 UK organisations representing children and young people, parents and the technology sector, is calling for a child rights-based approach to the development of digital technologies and support for children's online activity. This is a perspective CHIS strongly endorses.

Every child has the right to grow up in a healthy and safe environment, and the state is the final guarantor of that right. Internet companies have no exemption, nor do any of the socially responsible online enterprises ever try to claim one. On the contrary, as the organisations with the greatest repository of knowledge about how their online services work and how the wider internet operates, it is entirely understandable that these companies acknowledge and accept that they carry an extra layer of responsibility in this area.

[9] http://irights.uk/

The value of the internet for children

The internet[10] has become a pivotal technology in the modern world. Many different societies, on all continents, are benefiting from its development.

The internet provides a platform for games, connectivity, creativity and learning. These values attract hundreds of millions of children and young people worldwide.

Children who do not have ready and convenient access to the internet can be at a disadvantage, both at school and socially, when compared with children who do. CHIS therefore promotes safe and equal access to the benefits of the internet for all children and young people, in all parts of the world.

It is not helpful or desirable for the discussion about internet content and children always to be framed by reference to what is bad, harmful or dangerous. There ought to be just as much interest in the positive things the internet can bring to children's and young people's lives. As this idea gains wider acceptance, it will increasingly raise questions about whether or to what extent governments can rely solely on the market to ensure positive, educational and enjoyable content are available online and to ensure both parents and children are aware of such resources.

However, there is no escaping the fact that the internet can and does expose children and young people to risk of harm. Age-inappropriate material, sites promoting damaging behaviour like self-harm and "thinspiration", illegal content and sexual predators or bullies are some of the potential risks children face online. The impact of such exposure can be every bit as devastating as it would be offline and has led to tragic consequences for individual children and young people.

CHIS strongly believes in the potential of the internet to enrich and empower children and young people's lives.

[10] There are many ways the internet can be accessed: laptop, desktop, notebook-sized or handheld computers, through mobile phones, games consoles, personal digital assistants and TV. Rather than repeat this list throughout this document, unless the text states otherwise, all of these routes are relevant.

Support for parents and voluntary organisations

Parents and guardians need help and support to understand how children and young people use new technologies so they can ensure children and young people get the most out of it. Such support would also enable parents to build their child's resilience so that they can cope with the pressures of the internet. Schools and the internet industry have vital supporting roles to play here, and the voluntary sector is also key. Adoption agencies and fostering services also have a responsibility to provide training and support to their carers. Adopted children and those in care could be in a situation where birth families might pose a threat to their safety.

Internet companies need to recognise that their actions and policies have direct consequences for voluntary organisations that have been established to help children. For example, a change of policy in relation to privacy settings or in allowing conduct on a particular website can generate floods of calls or emails to helplines or voluntary services who are left to cope as best they can. Typically, they will not be resourced to meet sudden large upsurges in demand so the internet companies' actions can damage the quality of service the voluntary organisation can provide to the vulnerable children they support.

Summary of recommendations

Child abuse images[11]

1. Public confidence in the way child abuse images on the internet are dealt with within the UK, both by the internet industry and law enforcement, has been badly shaken. Revelations about the scale of offending – that is the number of people who seem to be willing to engage in the vile trade – and in the volume of images being circulated has caused this. Whatever we have all been doing so far, it is quite obviously not working well enough.

2. The government should initiate a major review of policy in this area which draws on expertise from a wide range of sources. The review should reflect on the role and responsibilities of all parts of the internet industry, law enforcement, the National Health Service and child protection agencies. There should be a special focus on how preventative technical and educational measures will contribute to a reduction in the scale of problem.

3. The rules of evidence and police procedures need to be updated to improve the efficiency and fairness of the processes associated with prosecuting cases involving child abuse images and videos.

4. The government should prepare a Bill that requires all UK-based communications service providers supplying internet access or services to members of the public – whether on a free or paid-for basis – to review whether or not their networks could be open to being abused by those who wish to store or transmit child abuse images. In the event that a communications service provider concludes that their network could be misused in this way, they will be further obliged to consider what reasonable steps could be taken by them to reduce or eliminate the risk of such abuse. The communications service provider will be required to publish the results of their analysis and any conclusions they reached.

5. The same Bill should require the Internet Watch Foundation (IWF) to publish a collated list on a regular basis of all communications service providers who are housing significant numbers of child abuse images. This provision should apply to all communications service providers, irrespective of where they are domiciled.[12]

6. To allow parents and other consumers to make an informed choice about their service provider, the IWF should publish a list of all UK-based communications service providers it has verified as using its blocking list.

7. An instruction should be issued to all government departments forbidding them from purchasing or using services from any communications service provider that appears on the list referred to in point 5 or does not appear on the list referred to in point 6.

8. Either through new legislation or existing administrative powers, the government should require all public sector agencies to adopt the policy outlined in point 7.

9. As part of the We Protect initiative within the Global Alliance, or in some other appropriate way, the government should promote discussions at an international level with a view to substantially improving the speed with which, once notified to the relevant authorities overseas, child abuse images on the internet are removed at source or access to them is denied. This is likely to require the creation of a new body to mediate between law enforcement and the internet industry.

[11] The term 'child abuse images' is used throughout this document to denote pictures or videos that are illegal under s.1 Protection of Children Act, 1978, as amended by s.84, Criminal Justice and Public Order Act, 1994 and s.41(1), Criminal Justice and Court Services Act, 2000, and s.160 Criminal Justice Act, 1988, as amended by ss.84(4) & 86(1), Criminal Justice and Public Order Act, 1994. Such images are otherwise referred to as indecent images of children, or historically as child pornography. This change in terminology reflects a growing awareness of the nature of the content typically found in these images and videos.

[12] OFCOM shall consult appropriate bodies to determine the basis on which a company would be named by the IWF.

10. The high-tech industries should urgently address ways to prevent the misuse of anonymity, encryption software and other technologies from facilitating the exchange of child abuse images and other kinds of online child abuse, for example via live streaming.

11. The high-tech industries should be encouraged to come up with new solutions to assist in or speed up the detection of new child abuse materials which have not yet been entered into databases established to assist law enforcement or communications service providers to combat the traffic to these images.

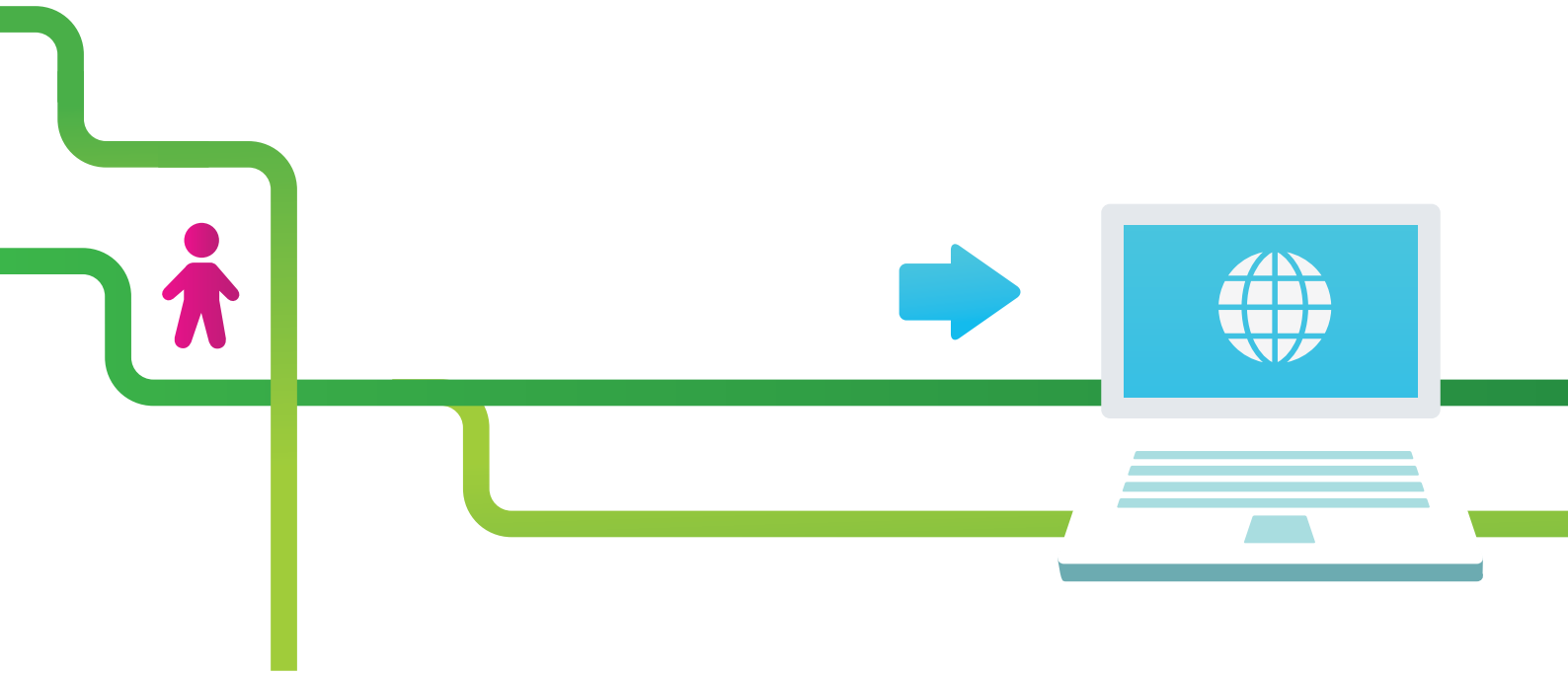
12. High-tech companies should be required to report child abuse material to the IWF and evidence of sexual grooming on their platforms to the police when they become aware of it.

13. The Treasury and the appropriate financial regulatory bodies should take a close look at the way pre-paid card systems and virtual systems such as Bitcoin might be fuelling criminal exchanges on the internet, particularly around child abuse images.

14. In order to promote more efficient blocking of child abuse websites worldwide, the UK government should engage with the EU and others with a view to expediting the creation of a single global list of all known online sources of child abuse materials, or a list that is as large as possible, including sites outside the EU. It should draw on any and all national lists that are not encumbered by local legal constraints. With appropriate security surrounding its deployment, this resource should be made available to all relevant online service providers, filtering companies and law enforcement agencies.

15. The UK government should establish, or help establish, a properly resourced special taskforce to work with INTERPOL, EUROPOL and other relevant police agencies to ensure the speediest possible development of a global database of hashes of known images of child abuse. It should be appropriately stratified so as to meet the legal and procedural needs of every jurisdiction that signs up to use it. The names of all participating forces should be published.

16. Under the EU's Data Protection Directive (95/46/EC, art 2.2.b) it is clear that publishing, disseminating, making available or hosting child sexual abuse images amounts to the processing of personal and sensitive data of a child. Yet within the EU, several companies are regularly found to have child abuse images stored on their servers. National Data Protection Authorities (DPAs) are responsible for monitoring the application of the Directive in their territory, but so far none have chosen to do so in respect of the prevalence of child abuse images on companies' servers. The DPAs should take a more active role in putting an end to the storing and dissemination of child sexual images in Europe. The UK government should promote discussion at EU level to see how this might best be achieved.



Research into child abuse images and grooming

17. The government should fund more research into the long-term consequences for, and therapeutic needs of, children who have been sexually abused generally, and when images of that abuse have appeared on the internet. The Child and Adolescent Mental Health Services could have an important role to play here. The government should ensure that appropriate resources are developed to address identified therapeutic needs and that the children's workforce is trained in how to use them and knows where to refer children so that they receive appropriate support.

18. The government should provide sufficient resources to help law enforcement achieve a higher rate of real world detection and location of victims who have appeared in child abuse images.

19. It is apparent from research that while everyone who downloads or collects child abuse images is a potential threat to children, not all collectors or downloaders are equally dangerous. This has important implications for decisions about resource allocation by law enforcement agencies, the prosecuting authorities, for sentencing policy, and the prison and probation services.

20. The government should fund research that will substantially enhance the diagnostic tools available to law enforcement and others to assist with decision making about individuals found in possession of child abuse images, or suspected of being in possession of them.

21. In particular, large-scale, authoritative research is needed to determine whether, or to what extent, there is a link between the offence of possessing child abuse images and committing other types of sexual offences against children. The research should also seek to establish if the possession of different types of child abuse images can be used to predict the future risk to children.

22. Research is also needed to establish the best strategies to deter people from viewing child abuse images online.

23. Research is needed to establish the best strategies to deter people from engaging in grooming behaviour online.

Online safety education

24. In order to inform the future design and implementation of educational resources to help children both stay safe online and make the best use of the internet, it is important that there is a full and independent research-based evaluation of current education and awareness programmes to determine what approaches are most effective. The same applies to programmes intended to reach out to parents and members of the children's workforce.

25. E-safety has been included across all key stages in the National Curriculum for computing in England since September 2013. Nevertheless, it seems likely that education about online child protection would be better placed in the Personal, Social and Health Education curriculum where it could be located within the wider context of children's and young people's real world lives.

Policing priorities

26. Much policing activity and related procedures should be re-orientated to recognise the central role that the internet and associated technologies play in a great deal of modern criminal behaviour, including many that put children and young people at risk. Every territorial police force should have a specialist resource to deal with sexual and other online offences against children. These officers should work closely with other relevant teams within their force.

27. Law enforcement agencies should be required to record all instances where the internet or new technology played a significant role in sexual abuse or other crimes involving children. This information should be recorded centrally by the Home Office. The data should include information about the age, and any other relevant characteristics, of the victims and the perpetrators, and their relationship to one another. It should also be published and broken down by reference to the constabulary area where the crime was committed.

28. Additional resources and a coordinated approach are urgently required to enable the police or other investigating authorities to improve the speed with which they can conduct forensic and other examinations of digital devices that are part of a criminal investigation into child abuse.

29. Media reports in 2014 disclosed that a teenager had been cautioned after sending a topless image of herself to her then boyfriend.[13] ACPO should reiterate and emphasise their 2012 guidelines[14] on young people who post self-taken images. Children and young people who engage in this type of behaviour typically need help, not a criminal record.

30. In March 2014, the Anti-Social Behaviour, Crime and Policing Act 2014 repealed the old system of Civil Prevention Orders and replaced them with two new orders: Sexual Harm Prevention Orders (SHPOs) and Sexual Risk Orders (SROs). These orders aim to provide enhanced protection for the public in the UK and children and vulnerable adults abroad, including from online offenders. We hope that both the police and courts will use the safeguarding opportunities presented by this new regime of civil orders to enhance the protection of children online, and that this is reflected in the forthcoming statutory guidance on the orders.

Public accountability

31. In 2013, Google and Microsoft made important changes to the way in which their search engines operate. These were aimed at reducing the scope for misuse of the search function for paedophilic purposes or to locate child abuse images and related materials. It appears from ad hoc media reports that these measures have been considerably successful, but it is important that systematic mechanisms are established to reassure parents and the public that the steps taken continue to work.

32. Similarly, other online service providers have given assurances that they are addressing a range of issues connected with children's online safety. But in practical terms there is no way anyone outside the company can know what, if anything, is being done or discover how well anything worked, or didn't. Companies typically refuse to disclose such information; often claiming it is commercially sensitive.

[13] J Tozer, "Schoolgirl cautioned for sending topless selfie to boyfriend as police warn sexting could leave children with criminal record", *The Daily Mail*. [Online] 14 July 2014, http://www.dailymail.co.uk/news/article-2702157/Sexting-leave-criminal-record-teenagers-told-Sharing-explicit-pictures-18s-illegal-taken-themselves.html [accessed 21 February 2015]. G Stubbs, "Schoolgirl given police caution after "sexting" explicit selfie to boyfriend", The Mirror [Online] 22 July 2014, http://www.mirror.co.uk/news/uk-news/schoolgirl-given-police-caution-after-3896649 [accessed 21 February 2014]

[14] Association of Chief Police Officers of England, Wales and Northern Ireland, *ACPO CPAI Lead's Position on Young People Who Post Self Taken Indecent Images* [Online] http://ceop.police.uk/Documents/ceopdocs/externaldocs/ACPO_Lead_position_on_Self_Taken_Images.pdf [accessed 21 February 2014]

33. The power and size of several internet companies, above all the combined outcome of inertia and the "network effect", means certain internet players are actual or quasi monopolies in a position which is not wholly dissimilar to that of a public utility.

34. The government should give urgent consideration to establishing mechanisms that would allow an appropriate degree of transparency in relation to online companies' behaviour where it concerns online child safety issues. Right now, a body that could undertake this kind of work does not exist, but Ofcom would be the closest to it. Perhaps a new division or department could be established within Ofcom to undertake work in this area. It ought to have the power to make legally binding rulings requiring internet companies to take necessary and proportionate measures to safeguard children online generally, and in respect of the position of children as economic actors and targets of advertising.

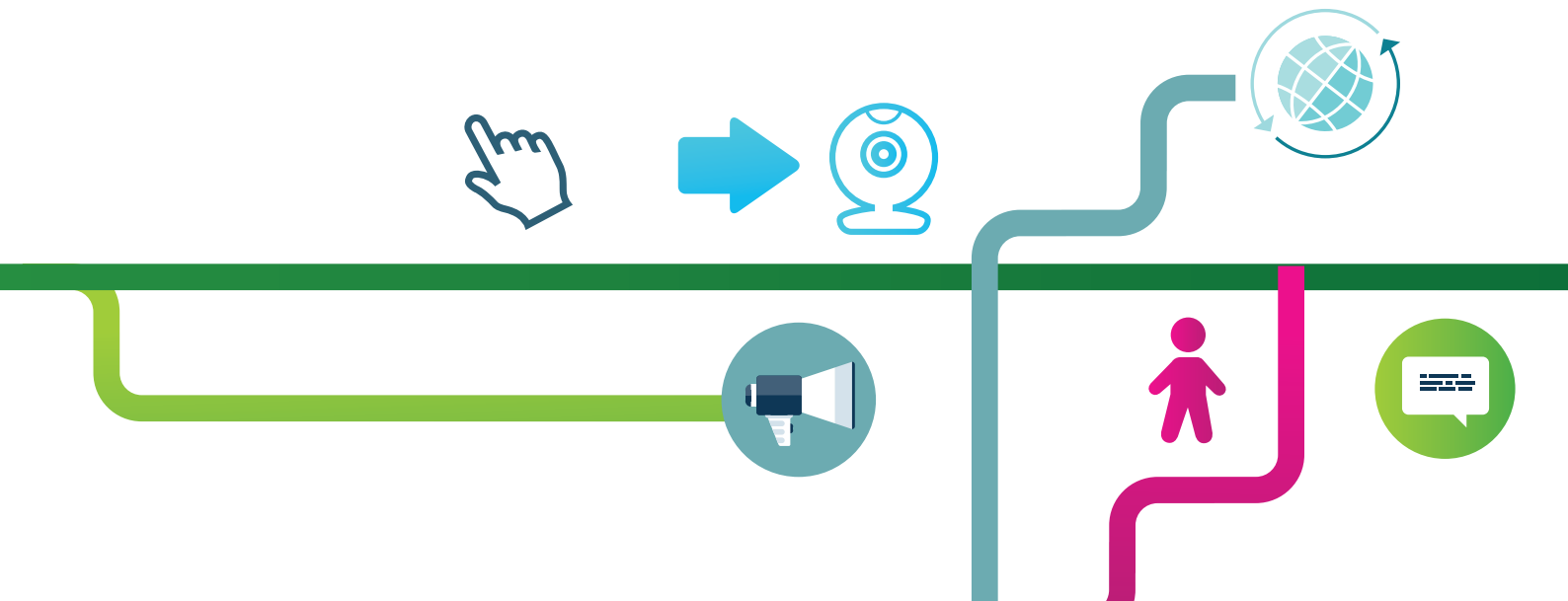
A new right for abused children

35. When a law enforcement agency becomes aware that any image of an identified and known child has been found in the unlawful possession of any third party and that third party is cautioned or convicted in relation to that unlawful possession, the law enforcement agency should, subject to there being no good reason not to, notify the child's parents or their legal representatives or, if they have reached the age of majority, the young person himself or herself providing they have indicated a desire to be so informed.

36. Following seizure of a child abuse image, the first priority for the police and related agencies must be to identify the child, determine their real life location and remove the child and other children who might also be at risk from the same offender to a place of greater safety, or to engage in some other type of intervention that puts the best interests of the child at the centre of and above all other considerations.

37. The government should consider the need for a new legal right for a child to obtain compensation from any person found to be in unlawful possession of an image of them that contravenes section 1 of the Protection of Children Act, 1978. This consideration should include (i) whether each person found in possession of an image should be considered jointly and severally liable for the full amount of the assessed damage suffered and compensation awarded and (ii) whether this right to obtain compensation should be extended to any identified child, irrespective of the country they live in, giving the child a cause of action within English courts.

38. In addition to paying compensation to individual children, consideration should be given to the need for an additional punitive element of damages which could be used to assist identified victims whose images have been found in the possession of impecunious criminals or for other beneficial purposes, for example to fund research in this area.



Data protection and access to age-restricted goods and services

39. The government should consider ways to ensure stricter compliance with the decision in R v Perrin (CCA 2002)[15] in respect of adult pornography sites. Perhaps the Gambling Commission's experience in certifying age verification systems could be brought to bear in this area. The Authority for Television on Demand's remit could be extended to enable them to advise or adjudicate on whether particular sites are covered by the decision in R v Perrin.

40. Legislation should be introduced to make it illegal for any bank, credit card company or other form of business or association to provide any services or facilities to companies or organisations that publish pornography on the internet but do not have a robust age verification process in place.

41. Legislation should be brought forward to provide for the development of regulations governing the online sale of age-restricted goods and services. It should be a crime for any bank, credit card company or other organisation to provide financial or other services to websites selling age-restricted goods or services without a robust age verification system in place.

42. The Information Commissioner's Office (ICO) should issue clear, research-based advice and guidance on the respective rights and responsibilities of all the parties where online data transactions involving children are concerned. These regulations should specifically address but not be limited to data transactions linked to the engagement of children in e-commerce.

43. In particular, the ICO should consider setting, or asking parliament to set, a legally defined minimum age below which verifiable parental consent will always be required in an online environment (though this should be balanced to avoid overly restricting the children's activities online). This should apply for all types of data transactions, or for those transactions linked to e-commerce, or both.

[15] Perrin, R v [2002] EWCA CRIM 747

Addressing future challenges of the mobile internet

44. The decision of the UK's major WiFi providers to restrict access to child abuse images and to legal adult pornography by introducing the "Friendly Wifi" scheme was a hugely important step which CHIS applauded.

However, CHIS remain concerned that there is no consistency to the standards being applied by the WiFi providers in terms of the legal adult content and services that they restrict. This potentially threatens the credibility and therefore the viability of the project. Moreover, CHIS is of the view that the Friendly WiFi scheme should more closely mirror the arrangements put in place by the mobile network operators where the BBFC plays a key role in advising on the age-appropriateness of content.

45. Relevant communication service providers should have a duty to report on their website, or another appropriate online space, whether or not they have taken up the Friendly WiFi scheme.

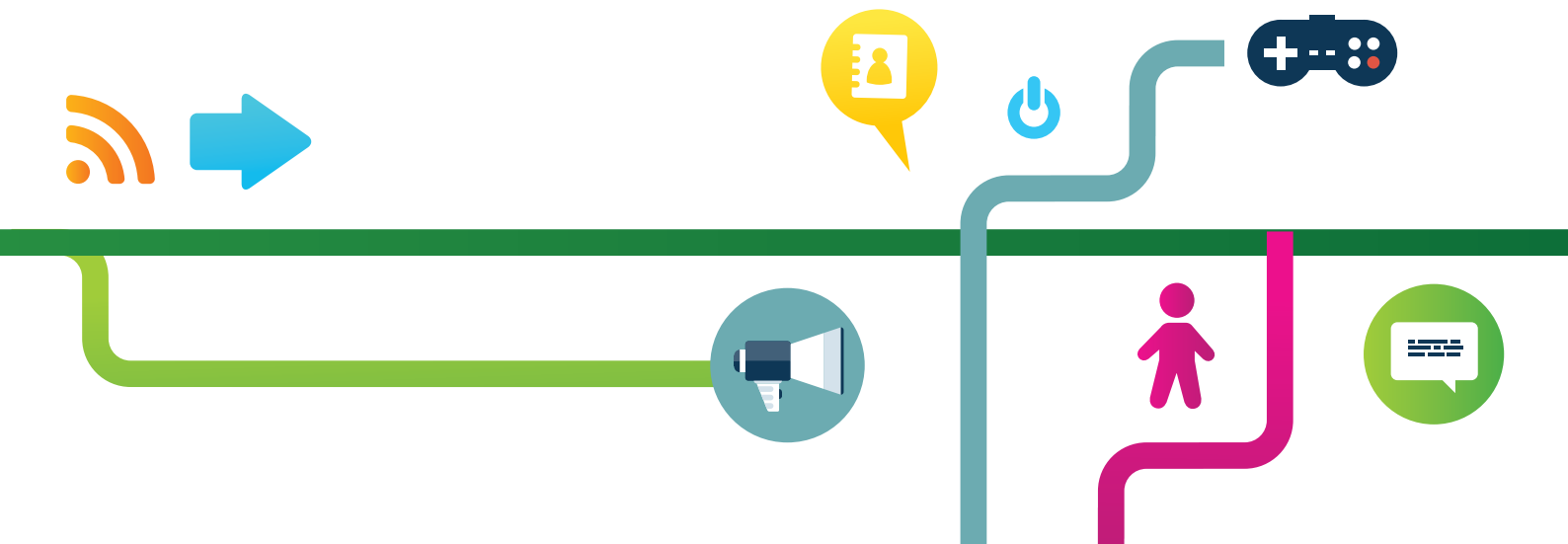
46. Mobile phone handset manufacturers and designers of operating systems for smart phones should accept a larger role in the ongoing discussions about child safety on the internet with a view to developing safety features that can operate by default and are integrated directly into the handsets.

47. Mobile phone handset manufacturers and network providers should consider developing devices designed specifically for children.

48. The government should initiate an inquiry into the new location technologies now emerging into the mass consumer market under the wider heading of the Internet of Things. Typically these technologies centre on or use mobile phone handsets, or other easily portable devices such as tablets or wearable devices. The inquiry should recommend what steps need to be taken to ensure that their services are marketed responsibly and that adequate security safeguards are in place to protect children and young people.

Advertising to children

49. A clear definition of what constitutes a website aimed primarily at children should be formulated and all advertising on such sites must conform to the Advertising Standard's Authority's Code of Advertising, Sales Promotion and Direct Marketing (CAP code).



Family safety software

50. The UK's ISPs took a tremendous step forward when they agreed to introduce filtering software to all of their customers, requiring them to decide whether or not they wished to use it.

We remain concerned that there is no consistency to the standards being applied by the ISPs, either in the way they present their offerings to parents or in terms of the categories of legal adult content they restrict. Different ISPs block different sites and this increases the risk of the idea that the ISPs' scheme risks over blocking. This potentially threatens the credibility and therefore the viability of the project. Moreover, CHIS is of the view that the ISPs' scheme should more closely mirror the arrangements put in place by the mobile network operators where the BBFC plays a key role in advising on the age appropriateness of content. This would create consistency across all three major modes of obtaining internet access (home, mobile and WiFi).

51. The level of take-up of the ISPs' "Active Choice" offerings needs to be monitored and reported on annually, including in respect of all ISPs active in the UK market, not only the "Big Four".

Support for professionals

52. The social work professions, youth workers, health service personnel and others who engage with children and young people need to become more closely engaged in the analysis of risks to children and young people on the internet and in the discussions about how best to provide some of the solutions. In particular, these groups need to be familiar with both the manifestations of online abuse in victims, and of the kinds of abuse perpetrators engage in. The professional bodies responsible for the accreditation of police, health, probation, prison staff, social workers, youth workers and teachers need to ensure that proper recognition is given within professional qualifications and professional development programmes about the importance of dealing appropriately with online offending or other related problematic behaviours. Similarly, adopters and foster carers need appropriate training and support to be best able to help keep their children safe online.

53. Appropriate advice should be available to all parts of the judiciary in relation to the nature and impact of the different types of online offending against children and young people.

Treatment provision

54. The Ministry of Justice, the Home Office, the Department of Health and other relevant agencies need to ensure that there is sufficient availability and take-up of treatment programmes for internet offenders. They also need to ensure that police and probation officers are appropriately trained to manage the risks posed by internet offenders, thereby minimising or reducing re-offences.

55. It is important that we develop a better understanding of both the range and spectrum of children's sexual behaviours online and how to assess and treat harmful sexual behaviours that are manifested in the online environment.

56. Appropriate assessment and treatment should be available for children displaying inappropriate or aggressive sexual behaviour online.

Social networking sites and online gaming

57. Ofcom has begun a process to develop new guidelines for the providers of social networking and other interactive services. This step is most welcome. However, in order for such guidelines to be fully effective and provide the public with the reassurance that the guidelines are being observed, a new body should be established, or a new division created within an existing one, which has the legal power to ensure internet companies are transparent and accountable in respect of actions aimed at supporting online child safety.

58. Such a body or division should also be given the power to make legally binding orders requiring internet companies to take necessary and proportionate measures to safeguard children online both generally and in respect of their position as economic actors and targets of advertising.

59. Social networking sites should ensure they have a mechanism to proactively identify and review content and services on their site, especially pictures and videos, and also ensure that they review all content reported to them within a clearly specified time period.

60. Playing online games remains an extremely popular activity with children of all ages. Like all aspects of the internet, online gaming can be a very positive experience for children, providing them with entertainment, education and opportunities to be creative. However, children are playing games against people they have not met in person. They may be living in jurisdictions with very different rules or expectations from ours.[16] Not all games producers pay sufficient attention to online safety issues. Every games producer needs to ensure effective safeguards exist within their games to eliminate or minimise the scope for anti-social behaviour. Every games producer needs to inform both gamers and their parents or guardians and teachers of the online safety issues in gaming.

Piracy websites

61. More needs to be done to ensure that parents, teachers and others in the children's workforce, and children and young people themselves, are aware of the role that many piracy websites play in drawing children and young people towards parts of the internet which are constructed and maintained by criminals, who not only profit from the unlawful sale of pirated materials, but are also a major source of age-inappropriate advertising. For example, advertising for prostitution, drugs, fake pharmaceuticals and software that is riddled with viruses that can takeover every device in the family home and defraud all or some household members.

[16] Ofcom, *Children and Parents: Media Use and Attitude Reports* [Online] October 2014, http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-use-attitudes-14/Childrens_2014_Report.pdf , p. 85, [accessed 09 March 2015]

Removing legal barriers

62. Efforts should be made to clarify the civil and criminal liabilities of ISPs and other online service providers in relation to user-generated content hosted on their websites. In particular, the government should press for an amendment to the E-Commerce Directive to remove any disincentive for internet companies to police their own sites for fear of attracting liability. ISPs and other online hosting companies should not lose the protection of 'mere conduit' status simply because they tried to locate and remove inappropriate or illegal content or content that contravened their terms of service. The principle should be that for liability to exist it is necessary to show an ISP or hosting company had actual knowledge of the illegal content and deliberately took no action or failed to act within a reasonable time.

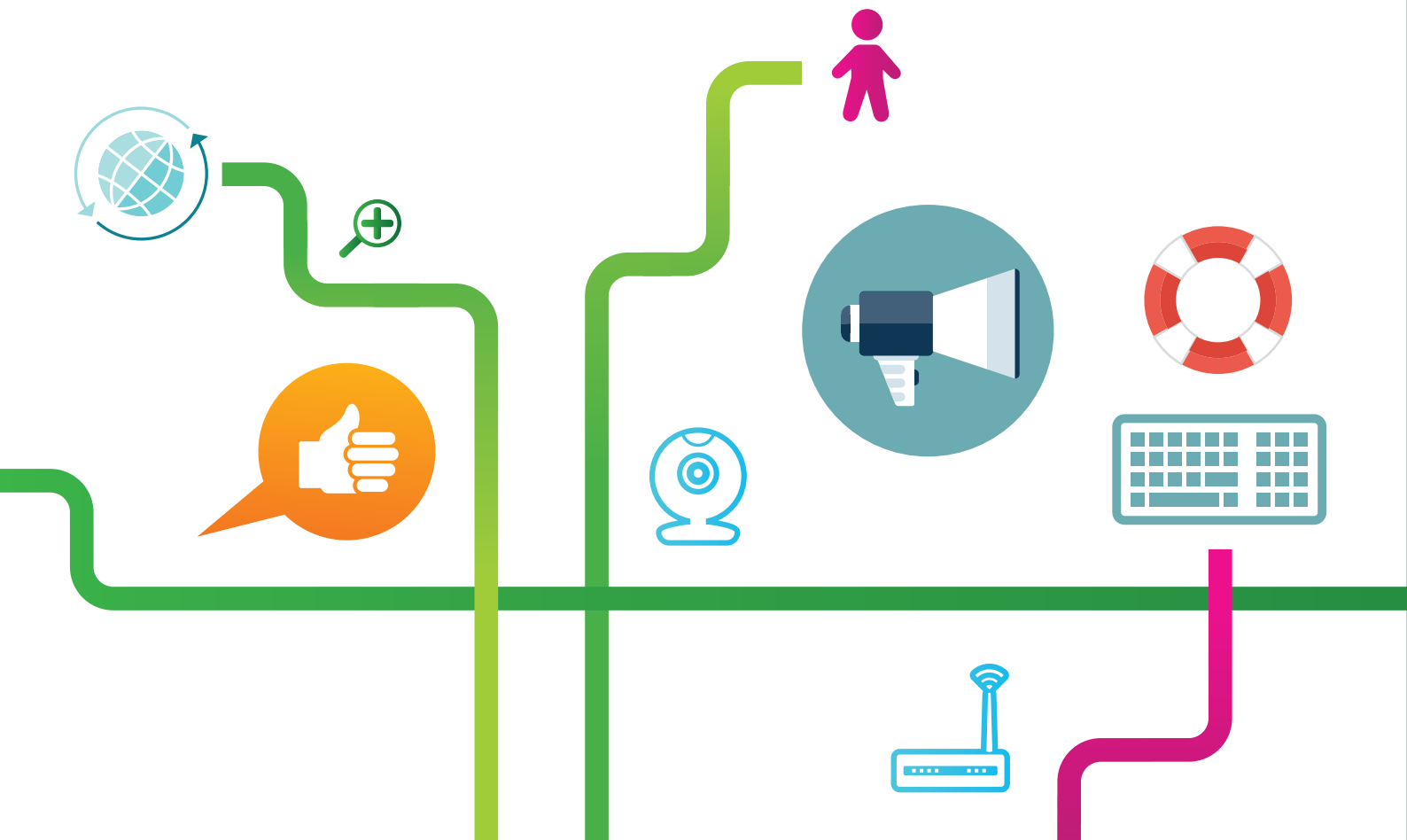
Future progress and policy development on internet safety

63. The government and law enforcement should seek to reduce their dependency on the internet and high-tech industries by developing their own independent sources of technical knowledge and expertise in these highly complex areas.

64. The government should find ways to help the third sector develop their own capacity to engage constructively and in a well-informed way, both nationally and internationally, with the consultative and other processes that are central to the development of policy in this area.

A high-tech social fund

65. Consideration should be given to establishing a special fund to which all high-tech companies will be encouraged to contribute. The fund will be independently administered and it will serve two purposes: to finance research into online child protection issues or concerns that are of a general nature and not specific to particular companies, and to be a place where voluntary bodies can go to seek funding for initiatives which arise directly or indirectly from changes to technology. In particular, CHIS foresees a need for considerable research and further thought around the emergence of the "internet of things" and wearable devices which can transmit location and other data.



Children's Charities' Coalition on Internet Safety

www.chis.org.uk

chisgb@outlook.com

10 Great Queen Street, London WC2B SDD